Dept of Broadband, Comms & Digital Economy

Submission on Digital Economy Future Directions Concept Paper

Version 0.3

Lockstep Technologies
11 February 2009

FOR PUBLIC RELEASE

Lockstep Technologies
Submission on Digital Economy Future Directions Concept Paper
Version 0.3
[Lockstep Submission on Digital Economy (0.3.1).doc]

FOR PUBLIC RELEASE

Table of Contents

1. Executive Summary

This submission on the Digital Economy Future Directions Concept Paper focuses on the issue of digital confidence.

The identity fraud epidemic and its implications for all online services must not be underestimated. The Internet has given criminals x-ray vision into peoples' banking details, and perfect digital disguises with which to defraud business and governments. Identity theft is perpetrated by sophisticated organised crime gangs, behind the backs of the best trained and best behaved online shoppers, aided and abetted by insiders corrupted by enormous rewards. No amount of security policy, database encryption or compliance audit can overcome the profit motives of today's fraudsters. The vulnerability of digital identities represents a real and present danger to the digital economy and therefore to the entire economy long term.

Lockstep contends that the predominant policy of technology neutrality and a focus on policy and user education has led to an imbalance in how government and business deals with identity security.

We urge government to treat cyber security – especially identity security – with the same sort of blended approach as befits any critical infrastructure, be it road, rail, telecommunications or electricity. We must move beyond education and awareness, to include standards, technology, and where necessary, regulation. In particular, government should lead by example, deploying the very best identity technologies to safeguard its citizens when rolling out coming generations of online services, such as health identifiers, shared electronic health records, social security services, and e-voting. We would like to see government and industry work in concert on a shared understanding of the digital identity problem and a uniform approach to its solution. A common approach does not imply a shared identity management *system*, which would be problematic on many levels. Rather, we advocate a shared set of standards and specifications – comparable to the telephony environment – underpinning a fully contestable market supplying solutions to all sectors.

Turning to Australia's competitiveness in the global digital economy, we start from the observation that, ironically, a great deal of digital confidence depends on material and geographical factors. The imperatives of massive new data centres and cross border flows of increasingly sensitive personal information bring with them enormous responsibilities for reliability, governance and transparency. Australia has special latent advantages in the race to meet these challenges, including a stable regulatory system, a privacy regime that happens to be in a period of reform, good ICT and Internet skills, and good international business relations. We close this submission with a high level and optimistic vision for how Australia could capitalise on its fortunate circumstances to take a leading role in building the worldwide digital economy.

2. Are we serious about online security?

This section is an edited version of Stephen Wilson's October 2008 column in Online Banking Review "Many hands make security work".

If one thinks about online security, all sorts of parallels emerge with other fields. A good comparison is road safety, which depends on a blend of user education, standards, processes and technological innovation.

Online safety is poorly served by the present preoccupation with user education. Numerous governments and industry groups have developed extensive and technically reasonable security advice.[1] But for the average Internet user, this material is probably overwhelming. There is a subtle implication that security is for experts, and that the Internet isn't safe unless you go to extremes. Moreover, the most recent cyber criminal attacks show that even if consumers do their best online, their personal details can still be taken over in massive raids on merchant databases.

We believe that too much onus is put by policy makers on regular users *protecting themselves* online, and that this creates a blind spot as to the possibility of active technological responses to the problem. In 2005, in relation to phishing, eBay's Hani Durzi said "I know that it sounds very basic, but education is the silver bullet".[2] Yet nobody would be so simplistic about road safety. As a community we accept that road safety rests evenly on enforceable road rules, legislated standards, quality automotive products, sophisticated traffic systems, and driver training and licensing. Education alone would be worthless.

In the aftermath of the TJ Maxx data breach (where tens of millions of credit card numbers were stolen by a gang that infiltrated department store networks), a column was headlined provocatively: "Preventing data breaches not a technology issue".[3] It may be politically correct to look beyond technology at these times, but it is ridiculous to ignore it. Nobody would ever assert that preventing bank robbery is 'not a technology issue'.

Credit card fraud and ID theft in general are in dire need of concerted technological responses. Our Card Not Present payments processing arrangements were developed many years ago for mail orders and telephone orders. It was perfectly natural to co-opt the same processes when the Internet arose, since it seemed simply to be just another communications medium. But the Internet turned out to be more than an extra channel: it connects everyone to everything, around the clock.

The Internet has given criminals x-ray vision into peoples' banking details, and perfect digital disguises with which to defraud online merchants.

[1] See for example www.protectfinancialid.org.au and www.staysmartonline.gov.au.

[2] Quoted in the New York Times, 7 March 2005.

[3] See http://www.networkworld.com/columnists/2008/062308insider.html.

There are opportunities for crime now that are both quantitatively and qualitatively radically different from what went before. In particular, because identity data is available by the terabyte and digital systems show no respect for originals versus copies, identity takeover is child's play.

You don't even need to have ever shopped online to run foul of CNP fraud. It is now apparent from TJ Maxx and other cases that most stolen credit card numbers might be obtained en masse by criminals invading databases at merchants' back-ends. These attacks go on behind the scenes, out of sight of even the most careful online customers.

So the standard cyber security advice increasingly misses the point. Consumers are told earnestly to look out for the SSL padlock that purportedly marks a site as "secure". They're supposed to have firewalls and to keep their PCs patched and up-to-date. They're advised to only shop online at reputable merchants and to avoid suspicious looking sites (as if cyber criminals aren't sufficiently organised to copy legitimate sites in their entirety). But none of this advice touches on the problem of coordinated massive heists of identity data.

Merchants too are on the hook for increasingly unwieldy and futile security overheads. When a business wishes to accept credit card payments, it's fair enough in the real world that they install certified terminal equipment. But to process credit cards online, shopkeepers now have to sign up to onerous PCI requirements that in effect require even SMEs become IT security specialists. But to what end? No audit regime will ever stop organised crime. To stem identity theft, we need to make stolen IDs less valuable.

All this points to urgent public policy matters for government and banks. It is not enough to put the onus on individuals to guard against one-off personal attacks on their credit cards. Systemic changes and technological innovation are needed to render stolen personal data useless to thieves. It's not that the whole payments processing system is broken; rather, it is vulnerable at one specific point.

Digital identities are literally the keys to our valuables. As such they really need to be treated as seriously as, say, house keys and car keys, which have become very high tech indeed. Modern car keys cannot be duplicated at a suburban locksmith; some office and filing cabinet keys even carry government security certifications. And we never use the same keys for our homes and offices; we wouldn't even consider it (which points to a basic oddity in the current craze for Single Sign On and identity "federation").

In stark contrast to car keys, there has been almost no attention paid to protecting digital identities. Our regulators' technology neutrality – bordering on technological timidity – has led to a bewildering array of stop-gap authentication approaches; at the same time we've done nothing to inhibit the re-use of stolen ID data. It's high time that all sectors reliant on the online channel got working together on a uniform and universal set of smart identity tools to protect consumers online.

3. Our perspective on Digital Confidence

The urgent need to neutralise identity theft

Identity theft is on the rise. In particular, large scale sophisticated raids by organised crime gangs on customer data bases are becoming more frequent. Two years ago, the networks of the TJ Maxx department store chain were infiltrated and records on some 94 million customers stolen. In late 2008, the payments processor Heartland Payments Systems suffered a breach of as yet unknown magnitude, but it is being reported as possibly the largest in history.

Stolen identity data is traded on a thriving black market, and is used in a range of criminal enterprises (including, it is thought, terrorism). The most overt identity crime is Card Not Present (CNP) payment fraud, where stolen credit card numbers and account details are replayed against unsuspecting e-merchants. Technically, this mode of cyber crime is child's play (it has to a large extent dwarfed the much more elaborate efforts needed to perpetrate Man in the Middle attacks on Internet banking sites). CNP fraud in Australia is the single biggest and fastest growing form of fraud; in FY2008 it cost AU$63M, accounting for 48% of all card fraud. The European Commission's Fraud Prevention Expert Group (FPEG) has reported that ID fraud has reached the point that it "undermines the general confidence in payments systems".

The limitations of perimeter security

By and large, government's response to public cyber security problems has been to focus on education and awareness campaigns (we will explore their limitations below). The only technologies that are promoted by government are conventional perimeter security measures: firewalls, anti-virus filters and hard-to-guess passwords (e.g. www.staysmartonline.gov.au). And yet identity theft tends not to occur while shoppers go about their business. Rather, most IDs are probably now obtained in carefully planned raids on backend data stores, chock full with account details from *all* retail commerce, not just e-commerce.

So, when criminals obtain customer details en masse, *they nullify all the best advice about how to be safe online*. A hapless customer need never have used their credit card online and still be defrauded when an attacker obtains their details and replays them in CNP Internet transactions. The well meaning guidance that consumers should only shop at reputable e-merchants, read the merchant's privacy policy, look out for the SSL padlock, and maintain their firewall and anti-virus software, is regrettably now almost entirely redundant.

The limitations of policy responses

The Concept Paper (p7) states that "recognising [the risk of identity theft] the Australian Privacy Commissioner released in August 2008 a Guide to Handling Personal Information Security Breaches that sets out protocols for agencies and organisations to prevent a data breach".

With the greatest respect to the Privacy Commissioner, their advice on this point, confined as it is to a comfort zone of policy and compliance, is increasingly meek in the face of the ID black market. The profit motive to obtain and trade IDs is so great that it will trump all policy-only responses. With millions of dollars to be made from stealing identity records, protocols and good practices are powerless.

Whenever sensitive data goes missing (as in the notorious UK Customs case, or when the ATO lost a CD last year[4]) there are earnest questions about whether the data was encrypted. Yet no commonly used commercial encryption method is likely to resist a concerted attack using the resources of organised crime, if there is millions of dollars worth of value to be gained. The discs that went missing from UK Customs were estimated to be worth in excess of one billion pounds on the black market.[5]

To really stop ID theft, we need proper technological preventative measures, not more policies and audits, and not more perimeter security. Stolen personal data should be rendered useless to thieves, to remove the profit motive for organised ID theft and neutralise the ID black market. There are well understood identity protections using smart devices (as deployed widely in the US government) that seem the only feasible way forward. The head of cryptography at NIST describes PKI smartcards in particular as "the only practical solution today [to account hijacking and eavesdropping]".[6]

The limitations of education

As mentioned, the modus operandi of organised cyber crime, in going behind customers' backs and stealing their IDs en masse from payment processors, department stores and so on, negate much of the online security advice given to consumers. We would like to go further now and point out some more fundamental limitations of trying to train lay people to behave safely on the Internet.

The medium itself is a big problem. There are really no reliable cues by which people can gauge real from fake online, or spot suspicious behaviours. For most people, the World Wide Web experience is much like watching a cartoon show on the TV. The human-machine interface is almost the same. The images and actions on the web are just as synthetic; crucially, *nothing on a web browser is real*. Almost anything goes – just as the

[4] See http://www.australianit.news.com.au/story/0,24897,24575839-15306,00.html.

[5] See http://news.bbc.co.uk/2/hi/uk_news/politics/7117291.stm.

[6] See http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf.

Roadrunner defies gravity in besting Coyote, there are no laws of physics that temper the way one web screen leads to the next. Therefore, many Internet users are probably liable to the same *suspension of disbelief* that enables the enjoyment of motion pictures.

So it is inevitable that people lose their bearings in the totally synthetic World Wide Web. Without realising it, they are taken in by a virtual reality, and become fatally vulnerable to social engineering.

Using the Internet "safely" today requires deep technical knowledge in order for the user to be able to abstract the different layers where threats may lurk. The requisite knowledge level seems to us to be comparable to the level of expertise needed to operate an automobile circa 1900. Back then a driver needed to know in depth how the machine worked so they could repair it in the back blocks. They had to maintain the engine (which we compare to configuring a PC operating system and firewall), watch out for dangers on the emergent road network (as often noted, there's no licensing on the Internet, nor any road rules), and even figure out how to fuel the contraption (the supply chains for Internet support services today are about as primitive as the petroleum industry was 100 years ago).

The Internet is so critical now that we need to move towards ways of working that don't require us to all be do-it-yourself experts.

The Concept Paper (p7) states that "Australians need to understand how to … protect personal information and identity online".

We would suggest that no amount of "understanding" can protect citizens against the newer and increasingly prevalent attack modalities. Even if you have never used your credit card online, you are vulnerable to CNP fraud because criminals steal account details en masse from card processors and large bricks-and-mortar stores. "Understanding" is moot when the consumer is powerless to prevent their details being taken behind their backs. The time has come for payment service providers to re-engineer their systems with better resistance to identity theft. Likewise, those that are planning online services in government need to take heed of ID theft in the finance sector, consider carefully the consequences for near term and medium term e-government programs, and implement real preventative measures to preserve the community's digital confidence.

The idea of digital identity infrastructure

Taken together, the tools and processes for managing digital identities could be regarded as critical infrastructure. Lockstep has published a detailed discussion of this previously, in a peer reviewed paper for the 2006 Homeland Security Summit (see References). The hallmarks of a worthwhile national approach to safeguarding identities include resistance to theft and replay, support for mutual authentication, ease of use, uniformity, interoperability, re-usability, and technological maturity. Note carefully that our vision is *not* for a shared identity management *system* but rather a shared understanding of the problem and a uniform approach to its solution, that leads to consistency with contestability.

4. Answers to selected questions in the DEFD paper

What more can industry and other stakeholders do to address concerns about consumer privacy and online safety?

Industry and government need to move beyond their preoccupation with security policy, management processes and compliance audit, and adopt a more blended approach in order to overcome the profit motives of today's fraudsters:

— In general, implement digital identity security measures that mitigate against abuse of stolen IDs, especially by replay attack

— make better use of smart devices to protect digital identity, such as those deployed in the US government

— make better use of smart devices to act as proxies for their users, protecting them from harm online, especially by automatically detecting illegitimate hyperlinks, spoof web sites, phishing, and spam.

What more can be done to increase trust and confidence in online transactions?

The Concept Paper actually says very little about the role of government in underpinning digital confidence. We urge government to treat cyber security with the same sort of blended approach as befits any critical infrastructure, be it road, rail, telecommunications or electricity. We must move beyond education and awareness, to include standards, technology, and where necessary, regulation.

Government should lead by example, deploying the very best identity technologies to safeguard its citizens when rolling out coming generations of online services, such as health identifiers, shared electronic health records, social security services, and e-voting.

Government must be prepared for identity theft to migrate into its own services, especially in respect of health identifiers. Medical identity theft for instance is already booming in the USA. Admittedly there are profit motives for fraudsters in the American system that are much larger than in Australia, but the phenomenon is inevitable here to some extent, even if only for mischief and blackmail. Banks can cover losses arising from financial identity theft, and can precisely recompense the victims, but the intangible losses arising from fraud against government services, and from medical privacy breaches are inestimably harder to compensate.

We would like to see a joint effort between government and industry to investigate, scope, specify and design a long term shared approach to national identity protection.

5. A vision for Australia's digital economy: *Pride of Place*

We attended the Digital Economy Capabilities Workshop in Sydney on 12 August 2008. At that time, an idea was generated that deserves further development; namely that *we could make Australia a worlds best practice digital economy and internationally preferred locale for setting up e-businesses*.

The idea arose as a synthesis of a large number of critical success factors for the digital economy which all related – ironically perhaps – to geographical and material factors. The workshop recognised the clear importance of regulatory frameworks, taxation, government policy, privacy, political stability, technological skills, climate and lifestyle.

Building on the realisation that physical place is still critical to the digital economy, Lockstep suggests that *an inspirational five year goal would be to make the dot-com-dot-au domain the best place in the world to set up e-businesses*. Recalling the Beijing ticketing fraud website, we see the potential for these scams to be made much more difficult to perpetrate in Australian domains.

We see a synthesis of regulatory and environmental characteristics coming together to make dot-com-dot-au the ideal location for online businesses:

— The current wave of privacy regime reforms could make Australia a better quality place to host, for argument's sake, health record servers than say California or India

— strong cyber security know how, in universities, government and the private sector, supported by existing clusters and associations

— good and rapidly improving broadband infrastructure

— good domestic technical skills

— historically excellent R&D skills

— good historical take-up of new technologies

— state and federal governments that are committed to innovation, ICT, broadband, know-how and the digital economy

— the presence of a great many global ICT players already

— a solid base of e-government readiness to build on

— great lifestyle and reputation to attract extra talent where needed.

There would be other critical prerequisites in the regulatory and taxation realms, to improve incentives for international businesses to establish operations here.

Appendix: About Lockstep Technologies

Lockstep Technologies researches and develops new solutions to identity theft and online fraud, centred on smartcards and Public Key Infrastructure (PKI). Sister company Lockstep Consulting provides independent advice, analysis and management consulting in cyber security policy and strategy, authentication and privacy.

Lockstep's recent government clients include Australia Post, the National eHealth Transition Authority, Medicare Australia, the Australian General Practice Network, and the Australian Government Information Management Office (AGIMO).

Lockstep founder and Managing Director Stephen Wilson recently served as an invited member of the Australian Law Reform Commission's Emerging Technology Subcommittee. He is currently a member of the Australian Industry Group (AiG) Digital Technologies Forum, the IT Testing Accreditation Advisory Committee of the National Association of Testing Authorities (NATA), and Standards Australia IT Security Subcommittee IT-12-4.

In October 2007 Lockstep Technologies was awarded an AusIndustry Commercialising Emerging Technologies (COMET) grant in support of our smartcard-based privacy and identity security products.

We have published widely on cyber security policy, privacy, e-health and related topics, and have previously made detailed submissions to government inquiries into the Human Services Access Card, the Privacy Act, spyware, and the draft national health privacy code.

See also www.lockstep.com.au/library.

References

[1]. Australian Payments Clearing Association *Fraud Perpetrated on Australian Issued Payment Instruments, 1 July 2007 – 30 June 2008* released December 2008;
available from www.apca.com.au.

[2]. European Commission Fraud Prevention Expert Group *Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan*, 22 April 2008;
http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf.

[3]. Stephen Wilson *Many hands make security work* Online Banking Review, October 2008.

[4]. Stephen Wilson *A new manifesto for smartcards as national information infrastructure* 5th Homeland Security Summit – 2006 Security Technology Conference, Canberra, 21 September 2006;
http://www.lockstep.com.au/library/smartcards/a_new_manifesto_for_smartcard.